CLAIMS

1. A security token, comprising:
   - a one-time password mechanism, for rendering one-time password functionality;
   - a public-key mechanism, for rendering public-key functionality with respect to said one-time password functionality; and
   - communication means for connecting said security token to said host and for providing to said security token the power supply required for operating at least said public-key mechanism.

2. A security token according to claim 1, further comprising a display, for displaying at least said one-time password.

3. A security token according to claim 1, further comprising a smartcard chip, for secure storage of keys and for rendering security-related functionality.

4. A security token according to claim 1, wherein said one-time password mechanism comprise means for generating a one-time value, said means selected from a group comprising: a real-time clock, and a counter.

5. A security token according to claim 1, wherein said communication means is selected from a group comprising: a display for displaying the password and thereafter manually providing the displayed value to a host, means for connecting said security token to said host via a wired connection, and means for connecting said security token to said host via a wireless connection.

6. A security token according to claim 5, wherein said wired communication means further comprise means for providing a power supply to said security token.

7. A security token according to claim 5, further comprising a chargeable power source, to be charged by the power supplied via said communication means, for providing the power for operating said security token while not connected to said host.

8. A one-time password security token, for securely providing a one-time value to a host system, said one-time password security token comprising:
   - means for generating said one-time value;
   - a public-key infrastructure mechanism, for performing public-key functionality with respect to said one-time value; and
   - communication means for connecting said security token with said host and for providing said encrypted one-time value to said host.

9. A one-time password security token according to claim 8, wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value by said public-key functionality, and digitally signing said one-time password.

10. A one-time password security token according to claim 8, further comprising a display, for displaying at least the encrypted one-time value.

11. A one-time password security token according to claim 8, further comprising a smartcard chip, for rendering security-related functionality.

12. A one-time password security token according to claim 8, wherein said one-time value is selected from a group comprising: the real-time, the value of a counter, and a group of random numbers.

13. A one-time password security token according to claim 8, wherein said communication means is selected from a group comprising: a display for displaying the password and thereafter manually providing the displayed value to said host, wired communication means with said host, wireless communication means with said host.

14. A one-time password security token according to claim 11, wherein said wired communication means further comprise means for providing a power supply to said security token.

15. A one-time password security token according to claim 8, further comprising a chargeable power source, to be charged by the power supplied by said communication means, for providing the power for operating said security token while not connected to said host.

16. A security system comprising:

- at least one security token comprising: a one-time password mechanism, for rendering one-time password functionality; a public-key mechanism, for rendering public-key functionality with respect to said one-time password functionality; and communication means for connecting said security token to said host and for

providing to said security token the power supply required for operating at least said public-key mechanism;

a host system, comprising: a one-time password mechanism, corresponding to the one-time password mechanism of said at least one security token, for rendering one-time password functionality; a public-key mechanism, corresponding to the public-key mechanism of said at least one security token, for rendering public-key functionality; communication means, corresponding to the communication means of said at least one security token, for communicating with said at least one security token and for providing to said token the power supply required for operating at least the public-key mechanism of said security token.

17. A system according to claim 16, wherein said communication means is selected from a group comprising: a display embedded within each of said at least one security token, for displaying the password and thereafter manually providing the displayed value to said host, wired communication means through which said at least one security token can be provided with the power supply required for performing public-key operations.

18. A system according to claim 16, wherein each of said at least one security token further comprising chargeable power source, to be charged via the power supply provided by said communication means, for providing the power for operating said at least one processor while not connected to said host, thereby enabling to operate said security token without external power supply.

19. A method for authenticating a client by a host system, said method comprising:

at said client side:

(a) generating a first one-time value;

(b) performing public-key functionality with respect to said one-time value;

(c) providing said value to said host system;

at said host system side:

(d) performing public-key functionality which corresponds to the public key functionality performed at step (b) with the provided value;

(e) generating a second one-time value in substantially the same manner as said first one-time value is generated;

authenticating said client by the correspondence of said second value to said first value.

20. A method according to claim 19, wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value, and digitally signing said one-time value.

21. A method according to claim 19, wherein said client is a security token.

22. A method according to claim 19, wherein providing the encrypted value to said host is carried out by a member of a group comprising: displaying said encrypted value at the client side and thereafter manually providing the displayed value to said host, means for connecting said security token to said host via a wired connection, and means for connecting said security token to said host via a wireless connection.